HCLSoftware

HCL **BigFix**
Cloud Lifecycle Management

Security Trust Center Document

Version 1.0

HCL has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the HCL website at www.hcltechsw.com.

Table of Contents

1 HCL BigFix Cloud Lifecycle Management Trust Center 6

1.1 Introduction 6

1.2 Security 6

1.2.1 Secure by Design 6

1.2.2 Identity and Access Management 6

1.2.3 Data Encryption 6

1.3 Secure Product Development 7

1.4 Secure distribution of binary 7

1.4.1 Platform Architecture and Multi-Tenancy 8

1.4.2 Security Incident Response and Bulletins 8

1.5 Scalability and Availability 8

1.6 Privacy 8

2 Conclusion 10

3 Support 11

Table of Figures

Figure 1 – Highly Secure Controlled Location 7

Document Revision History

This document is updated with each release of the product or when necessary.

This table provides the revision history of this Security Trust Centre document .

Version Date	Description
September, 2025	HCL_BigFix_Cloud_Lifecycle_Management_Trust Centre_v1.0

1 HCL BigFix Cloud Lifecycle Management Trust Center

1.1 Introduction

At HCLSoftware, we are fundamentally committed to earning and maintaining your trust, Security, privacy, and compliance are the foundations of our products. The HCLSoftware security strategy covers all aspects of our business, including corporate and organizational security policies, incident management and response, business continuity and disaster recovery, secure software development processes, and privacy.

This Trust Centre provides a transparent overview of the principles and practices governing HCL BigFix Cloud Lifecycle Management, giving you the confidence to manage your hybrid-cloud environments with our platform.

1.2 Security

We integrate security into every phase of the product lifecycle, from concept to deployment, to protect your data and infrastructure.

1.2.1 Secure by Design

HCL BigFix Cloud Lifecycle Management is developed in-house following a secure software development lifecycle. The product undergoes a comprehensive threat modeling assessment to proactively identify, evaluate, and mitigate potential security risks from the ground up.

1.2.2 Identity and Access Management

- **Authentication:** Access is protected out-of-the-box with role-based access controls. For enhanced security, we strongly recommend integrating your instance with a **SAML 2.0 Identity Provider (IdP)** like Azure AD or Okta. This enables Single Sign-On (SSO) and gives you full control over password policies and the ability to enforce **Multi-Factor Authentication (MFA)**. The platform can also integrate with external data stores like LDAP (Active Directory Authentication)
- **Authorization:** After successful authentication, user permissions are managed by roles under the principle of least privilege. BigFix Cloud Lifecycle Management provides out-of-the-box roles (e.g., provider, requestor, organization admins, business approver, IT admin) that can be assigned to users or groups to control access to specific product features and data based on user persona.

1.2.3 Data Encryption

We employ strong, industry-standard encryption protocols to protect your data at all stages.

- **Encryption in Transit:** All access to your instance over the internet is encrypted using **Transport Layer Security (TLS) with TLS1.2 cipher suites**. All HTTP requests are automatically redirected to HTTPS. We also recommend using encryptions for all integrations.
- **Encryption at Rest:** Data stored in the underlying database, along with all automated backups, is encrypted using **AES-GCM-256**.

1.3 Secure Product Development

HCLSoftware adheres to stringent development processes to produce the code we develop and provide to our customers. All Development practices incorporate change control and are the key criteria assessed at release approval stage including key practices around following

- **Threat Modeling** - Threat modeling is the process of identifying and prioritizing potential threats to a system and finding solutions to mitigate them.
- **Secure Design Review** - Secure Design Review is an assessment done for a product by the HCLSoftware Security team to understand the product architecture, means of deployment / delivery and various other security measures which are in place, as per the industry standards
- **Data Privacy Assessment** - HCLSoftware's Privacy and Data Protection by Design and Default (PbD for short) addresses privacy requirements to meet those laws and regulations and asks all product teams to work with these requirements in the design phase and test them in the verification phase of the development project. HCL Software leverages the One Trust Platform to perform Data Privacy assessments for products, platforms and Operations Support
    - Static and Dynamic Application Security Testing
    - Code Quality Analysis
    - Open-Source Code Composition and Vulnerability Analysis
    - Penetration Testing - Performed by Internal (for every release) and External (once in calendar year) teams.

Figure 1 – Highly Secure Controlled Environment

1.4 Secure distribution of binary

The binaries for the product are securely distributed via MHS Portal. My HCLSoftware (MHS) is a web application for HCLSoftware customers and partners that provides a new and improved way to find and quickly download the latest HCLSoftware product releases as well as supported older releases. All binaries are cryptographically signed. MHS provides seamless access to resources and tools designed to effectively manage the use of HCLSoftware products and services.

- Active license enforcement
- Usage metering and reporting
- Access-controlled content: users only see content appropriate for them
- Enables seamless access to resources and tools to help effectively manage the entire HCLSoftware experience

1.4.1 Platform Architecture and Multi-Tenancy

The platform is built with multi-tenancy by design, making it ideal for Managed Service Providers (MSPs) and Shared Service Organizations. Each customer's data resides in a logically separated space, segregated by a unique tenant/provider record to ensure data cannot be viewed by another customer, preventing data co-mingling.

1.4.2 Security Incident Response and Bulletins

The **HCL Product Security Incident Response Team (PSIRT)** manages the receipt, investigation, and internal coordination of reported security vulnerabilities for HCL Software product offerings. The PSIRT coordinates with product development teams who investigate reported vulnerabilities and identify the appropriate response plan. For more information, visit the HCLSoftware PSIRT page.

The HCL PSIRT publishes Security Bulletins describing any relevant CVEs and pointing to additional details and remediation. A list of security bulletins for HCL BigFix CLM can be found on the official HCL Software support and community forums.

1.5 Scalability and Availability

Our platform is engineered for high availability and business continuity, protecting your operations from disruption.

- HCL BigFix CLM is designed with scalability and reliability at its core. The platform can seamlessly scale based on the number of virtual machines (VMs) that need to be managed, ensuring consistent performance regardless of workload size.
- All internal components of the system are built to support **high availability**. This is achieved through load balancing across services, which eliminates single points of failure and ensures continuous service uptime even under high demand or during component failures.

1.6 Privacy

- **Data Roles and Responsibilities:** In our relationship, the **customer is the data controller**, retaining full ownership and control over the data collected and determining the purpose of its use. For more information visit HCL Software Privacy
- **Purpose Limitation and Data Minimization:** The platform is designed to process personal data for the sole purpose of product administration and fulfilling our contractual obligations. We practice data minimization, and the product is not designed to process any special categories of sensitive personal data.

- **Customer Information Processed:** The platform may process the following customer information as part of its standard functionality:
  - **Contact Information:** Organisational Email Address
  - **Personal Identification:** First Name, Full Name, Last Name
  - **User Account Information:** Login ID
  - **Technical Metadata:** Browsing Time, IP Address

2 Conclusion

Our valued clients can rest assured that we keep security foremost in our minds as we develop, test, and deliver effective and secure solutions to our customers.

3 Support

For more information and related queries drop an email to BigFixCLM-PS-Team@hcl-software.com.

HCLSoftware

hcltechsw.com